UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/859,429	05/18/2001	Makoto Kayashima	566.39530VX1	5340

24956 7590 08/20/2008

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/859,429	KAYASHIMA ET AL.	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/761,742.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/1-2-2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 1-13 are cancelled. Applicant's arguments/amendments with respect to pending claims 14-18 filed 5/12/2008 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Information Disclosure Statement

The information disclosure statement filed 1/2/2008 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because a translation of (at least) the abstract of reference 'A' under the "Other Documents" section has not been provided by applicants. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 14-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beebe et al., United States Patent No. 6,226,372, and further in view of Depaolantonio, US Patent No. 6,950,865.

As per claim 14:

Beebe et al. substantially teach a security management method comprising: designing security specifications to be applied to the information system by using an information security policy designated by a user (col. 8, lines 18-40), wherein the information security policy is applied to each of the plurality of managed systems designated by the user (col. 8, line 41 – col. 9, line 21 and col. 10, lines 19-25), wherein the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures (col. 9, lines 22-36), and wherein each security measure indicates an action for be taken to secure the managed systems (col. 10, lines 44-58); auditing a security status of the information system with respect to the information security policy designated by the user, wherein the security status indicates whether a security measure has been executed (col. 9, lines 37-51); changing the security status of each of the managed systems based on a result of auditing the security status (col. 9, lines 52-67); and auditing the security status of the information system every time a security setting is changed (col. 11, lines 12-26).

Not explicitly disclosed is auditing system information of each of the plurality of managed systems, wherein the system information comprises a version of a software program installed in each respective management system, and a type of apparatus in which each respective managed system operates, and wherein the system information changes along with the security status information. However, Depaolantonio teaches that several forms of system data can be collected and used in reference to various managed systems within a network, where the configuration information and device type are included in the information to be audited (col. 4, line 54 - col. 5, line 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Beebe et al. to audit system information regarding the hardware/software configurations of each of the managed systems with information regarding the type of device, as well as to use this information in changing the security status of the system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Depaolantonio suggest that collecting information regarding the flow of particular devices with particular configurations allows for a more proper assessment of the devices which are active within the network in col. 5, lines 46-67.

As per claim 15:

Beebe et al. and Depaolantonio substantially teach the method of claim 14. Furthermore, Beebe et al. teach the method further comprising: diagnosing the security of the information system by using an audit program selected from a second database, which includes a correspondence between audit programs, the information security policies, the managed systems, and management programs (col. 11, lines 40-53), wherein each audit program audits the security

status of each of said managed systems (col. 11, lines 40-53), and wherein the management programs manage security measures of the information security policies and are designated by the user when performing the step of designing the security specifications (col. 11, lines 53-61); and changing, by a management program selected from the second database, the security status of a managed system corresponding to the management program, so as to adjust the security status in accordance with an information security policy corresponding to the management program (col. 11, line 62 – col. 12, line 15).

As per claim 16:

Beebe et al. and Depaolantonio substantially teach the method of claim 14. Furthermore, Beebe et al. teach the method further comprising: in accordance with a security setting content received from the user, changing, by a management program selected from a second database, the security status of a managed system corresponding to the management program, so as to adjust the security status in accordance with the information security policy corresponding to the management program (col. 11, lines 40-53), wherein the second database includes a correspondence between audit programs, the information security policies, the managed systems, and management programs (col. 11, line 62- col. 12, line 15).

As per claim 18:

Beebe et al. substantially teach a security management system comprising: a first database, which includes information regarding the managed systems to which information security policies are applied (col. 12, lines 36-39 and col. 17, lines 27-31); a second database, which includes information regarding specifications of information security policies (col. 12, lines 39-41 and col. 13, lines 56-65); a third database, which includes a correspondence between

the managed systems and information security policies (col. 12, lines 41-43 and col. 17, lines 27-31); a management and audit object area control section which selects, from said first database, managed systems to which information security polices are applied based on a designation by a user (col. 12, lines 44-54); an information security policy selection control section which extracts, from said second database, information security policy specifications based on a designation by a user (col. 12, lines 54-65); an information security policy/security management and audit program correspondence control section that extracts, from said third database, an information security policy corresponding to the managed systems, and designs security specifications for each of the managed systems by using the information security policy specifications designated by the user (col. 12, line 66 – col. 13, line 7); a plurality of audit sections that audit a security status of the information system with respect to the information security policy designated by the user (col. 13, lines 8-22), wherein the security status indicates whether a specific action to secure the managed systems has been executed (col. 13, lines 22-24); and a plurality of management sections that obtain the security status of the information system, based on audit results from the plurality of audit sections, and manage security status relating to the information security policy of the managed systems in order to bring the security status of the managed systems in conformity with the information security policy specified by the security specification designed at the information security policy/security management and audit program correspondence control section (col. 13, lines 24-26), wherein the information security policy/security management and audit program correspondence control section audits the security status of the information system every time a security setting is changed (col. 19, lines 23-44).

Not explicitly disclosed is auditing system information of each of the plurality of managed systems, wherein the system information comprises a version of a software program installed in each respective management system, and a type of apparatus in which each respective managed system operates, and wherein the system information changes along with the security status information. However, Depaolantonio teaches that several forms of system data can be collected and used in reference to various managed systems within a network, where the configuration information and device type are included in the information to be audited (col. 4, line 54 - col. 5, line 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Beebe et al. to audit system information regarding the hardware/software configurations of each of the managed systems with information regarding the type of device, as well as to use this information in changing the security status of the system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Depaolantonio suggest that collecting information regarding the flow of particular devices with particular configurations allows for a more proper assessment of the devices which are active within the network in col. 5, lines 46-67.

III. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Beebe et al., United States Patent No. 6,226,372 and Depaolantonio, US Patent No. 6,950,865 as applied to claim 14 above and further in view of CERT's CC Vendor-Initiated Bulletins 1994-1998.

As per claim 12:

Beebe et al. and Depaolantonio substantially teach the security management method according to claim 14. Not explicitly disclosed is checking the result of auditing against security

hole information published by a security information organization to determine if a security hole exists; and changing the security status of the managed system in which a security hole is found. However, CERT/CC Vendor–Initiated Bulletins disclose security hole information published by a security information organization including CERT. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Beebe et al. to incorporate the use of security hole information published by a security information organization. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since CERT/CC Vendor –Initiated Bulletins 1994-1998 suggest that it is very important to deal with security vulnerabilities as soon as possible which means that it is necessary to report vulnerabilities as discovered in order to allow all users to take the necessary precautions in pages 1-8.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,990,591
2. US Patent No. 7,020,697
3. US Patent No. 6,115,735
4. US Patent No. 6,216,231
5. US Patent No. 6,678,827
6. US Patent No. 6,532,543
7. US Patent No. 5,859,966
8. US Patent No. 6,353,886

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2137
8/14/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137